



**BOX AF**  
JONES and Mal.

**PATENT APPLICATION**

**RESPONSE UNDER 37 CFR §1.116  
EXPEDITED PROCEDURE  
TECHNOLOGY CENTER ART UNIT 2134**

AF  
2134

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Ryuichi AOKI

Group Art Unit: 2134

Application No.: 09/415,461

Examiner: P. Callahan

Filed: October 14, 1999

Docket No.: 104526

For: APPARATUS AND METHOD FOR DEPOSITING ENCRYPTION KEYS

**REQUEST FOR RECONSIDERATION AFTER FINAL REJECTION  
UNDER 37 CFR §1.116**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RECEIVED**

MAY 26 2004

Technology Center 2100

Sir:

In reply to the March 24, 2004 Office Action, reconsideration of the rejections is respectfully requested in light of the following remarks.

Claims 1-3 and 5-29 are pending in this application. Applicant appreciates the Office Action's indication that claims 9-11, 14, 20-22 and 27-29 contain allowable subject matter.

Applicant thanks Examiner Callahan for the courtesies extended to Applicant's representative, Mr. Luo, during the May 14, 2004 personal interview. The substance of the personal interview is incorporated in the following remarks.

**I. The Claims Satisfy All Requirements Under 35 U.S.C. §112, Second Paragraph**

The Office Action rejects claims 1, 12, 13 and 15 under 35 U.S.C. §112, second paragraph. This rejection is respectfully traversed.

The Office Action asserts that it is unclear from the language of the claims whether the Applicant contemplates the depositaries as discrete entities or as resident storage areas or modules on a server. The Office Action further asserts that the arrangements of elements in the apparatus is not clearly illustrated in the drawings. Applicant respectfully submits that the claims satisfy all requirements under 35 U.S.C. §112, second paragraph.

An exemplary depositary is described in the specification and shown in the drawings. For example, in an exemplary embodiment, the depositary may be a client. See the specification at, for example, Fig. 1, and page 9, lines 1-2.

In particular, at page 9, lines 1-2, the depositary is referred to as an entity with which a private key of an individual is deposited. In Fig. 1, clients 200 include a private secondary storage 201 in which an individual's private key is shown.

Furthermore, the claims need to claim the subject matter which the Applicant regards as his invention. 35 U.S.C. §112, second paragraph (emphasis added). What needs to be included in the claims is what is "necessary to practice the invention." See MPEP §2172.01. As discussed during the personal interview, the subject matter recited in claims 1, 12, 13 and 15 is not limited to whether the depositary is a discrete entity or as resident storage areas or modules on the server. Thus, whether the depositary is a discrete entity is not required to be included in the claims. The claims should be construed to cover either case, since Applicant is entitled to cover either case absent anticipation or obviousness of such in view of the prior art.

For at least the above reasons, the claims satisfy all requirements under 35 U.S.C. §112, second paragraph. Accordingly, withdrawal of the rejection of claims 1, 12, 13 and 15 under 35 U.S.C. §112, second paragraph is respectfully requested.

**II. The Claims Overcome the Rejection Under 35 U.S.C. §102**

The Office Action rejects claims 1-3, 5, 7, 12, 13, 15, 16, 18 and 23-26 under 35 U.S.C. §102(b) over U.S. Patent No. 5,436,972 to Fischer. This rejection is respectfully traversed.

The Office Action asserts that Fischer discloses all elements recited in claims 1-3, 5, 7, 12, 13, 15, 16, 18 and 23-26. Applicant respectfully submits that Fischer does not disclose or suggest a server that, in response to a recovery request from a depositary, sends to the depositary the recovery information encrypted by a public key of the depositary, and acquires from the depositary the recovery information decrypted by a private key of the depositary and then encrypted by a public key of the server, as recited in claims 1-3, 5, 7, 12, 13, 15, 16, 18 and 23-26.

As discussed during the personal interview, Fischer does not disclose or suggest sending the recovery information that is encrypted by a public key. Moreover, Fischer does not disclose or suggest sending the recovery information encrypted by a public key of the depositary, and acquiring the recovery information that is decrypted by a private key and then encrypted by a public key of the server.

In particular, Fischer discloses an escrowed secret information retrieval scheme in which a trustee evaluates a retrieval request from an Applicant. See col. 10, lines 49-54. The Applicant is required to submit an escrow information record 80 and documentation containing credentials which can be used to verify that the Applicant is the legitimate owner of the secret information. See col. 10, lines 54-63. The escrow information record 80 has already been encrypted in a definition phase prior to the retrieval phase. See col. 9, lines 8-11, and col. 10, lines 24-27. The escrow information record is not encrypted during the retrieval phase.

As discussed during the personal interview, Fischer discloses that the documentation contains credentials such as an affidavit executed by a Notary Public attesting to the Applicant's characteristics. See col. 10, lines 60-66. This documentation is not encrypted, but is to be compared with standard escrow information submitted in the definition phase. See Fig. 2 and col. 7, lines 7-34. As discussed during the personal interview, nowhere does Fischer disclose or suggest sending the recovery information that is encrypted by a public key of the depositary. Nowhere does Fischer disclose or suggest acquiring recovery information decrypted by a private key of the requestor or depositary, and then encrypted by a public key. Therefore, Fischer does not disclose or suggest a server that, in response to a recovery request from a depositary, sends to the depositary the recovery information encrypted by a public key of the depositary, and acquires from the depositary the recovery information decrypted by a private key of the depositary and then encrypted by a public key of the server, as recited in claims 1-3, 5, 7, 12, 13, 15, 16, 18 and 23-26.

For at least the above reasons, Fischer does not disclose each and every element recited in claims 1-3, 5, 7, 12, 13, 15, 16, 18 and 23-26. Therefore, Fischer does not disclose or suggest the subject matter recited in claims 1-3, 5, 7, 12, 13, 15, 16, 18 and 23-26. Accordingly, withdrawal of the rejection of claims 1-3, 5, 7, 12, 13, 15, 16, 18 and 23-26 under 35 U.S.C. §102(b) is respectfully requested.

The Office Action rejects claims 6, 8, 17 and 19 under 35 U.S.C. §103(a) over Fischer and Official Notice. This rejection is respectfully traversed.

The Office Action recognizes that Fischer does not disclose or suggest a server log for recovery requests. However, the Office Action takes Official Notice that this feature is well known in the art. Applicant respectfully submits that the Official Notice does not disclose or suggest sending recovery information encrypted by a public key of the depositary, or acquiring the recovery information that is decrypted using a private key of the depositary and

then encrypted by a public key of the server. Therefore, the Official Notice does not supply the subject matter lacking in Fischer. Additionally, if the Patent Office intends to continue relying on Office Notice, Applicant respectfully requests that a reference be provided to show the allegedly old and well known feature.

For at least the above reasons, Fischer and the Official Notice, either individually or in combination, do not disclose or suggest the subject matter recited in claims 1 and 12 and claims 6, 8, 17 and 19 depending therefrom. Withdrawal of the rejection of claims 6, 8, 17 and 19 under 35 U.S.C. §103(a) is respectfully requested.

### **III. Conclusion**

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,



James A. Oliff  
Registration No. 27,075

Gang Luo  
Registration No. 50,559

JAO:GXL/sqb  
Date: May 24, 2004

**OLIFF & BERRIDGE, PLC**  
**P.O. Box 19928**  
**Alexandria, Virginia 22320**  
**Telephone: (703) 836-6400**

<p><b>DEPOSIT ACCOUNT USE AUTHORIZATION</b> Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461</p>
---